Information Assurance (IA)
Frequently Asked Questions (FAQs)

Version 1.0

Table of Contents

Information Assurance (IA)
Frequently Asked Questions (FAQs)

Can I bypass Information Assurance activities by leveraging non-cloud, as opposed to cloud, services or by acquiring services myself rather than going through the Broker?

No. DoD Information Assurance, NetOps, and Computer Network Defense policies apply to operation and use of all cloud and non-cloud IT infrastructure, platform, and software services and applications and apply regardless of how the acquisition is accomplished.

Is there any guidance that applies specifically to use of commercial cloud services?

Yes. Per the 9 December 2011 "Interim Guidance Memorandum on Use of Commercial Cloud Computing Services", "...use of third party, off-premises cloud services will require a waiver from the GIG Waiver Panel in order to preserve the security of DoD data and mission assurance in the face of persistent cyber threats from capable adversaries".

Are there any considerations related to commercial cloud services that preclude me from doing a full and open acquisition?

There are no considerations that preclude such an acquisition. However, you should take the required certification and accreditation activities into account in your acquisition planning. Based on current policies, it may take considerable time and effort for a vendor to get the required support infrastructure in place to meet the monitoring and reporting requirements for Controlled Unclassified Data (including Personally Identifiable Information and Protected Health Information).

Are there any special considerations related to use of Software as a Service?

Yes. For Software as a Service (SaaS), the entire stack (infrastructure, platform, and software) must be accredited before implementation. If the SaaS is going to operate on a previously accredited infrastructure, the timeline for certification and accreditation may be shorter than if the entire stack is being assessed for the first time.

What policy and other documents are relevant to Information Assurance and use of cloud services by DoD?

➢ CJCSM 6510.01B: Chairman of the Joint Chiefs of Staff Manual: Cyber Incident Handling Program, dated 10 July 2012.
http://www.dtic.mil/cjcs_directives/cdata/unlimit/m651001.pdf

➢ CNSSI 1253: Security Categorization and Control Selection for National Security Systems, dated 15 March 2012.
http://www.cnss.gov/Assets/pdf/Final_CNSSI_1253.pdf

➢ CNSSI 4009: National Information Assurance (IA) Glossary, dated 26 April 2010.
http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

➢ Executive Order 13526: Classified National Security Information, dated 29 December 2009.
http://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information

➢ DoD Chief Information Officer, Designation of the Defense Information Systems Agency as the Department of Defense Enterprise Cloud Service Broker, dated 26 June 2012.
http://www.disa.mil/Services/DoD-Cloud-Broker/~/media/Files/DISA/Services/Cloud-Broker/disa-designation-memo.pdf

➢ DoD Chief Information Officer, Interim Guidance Memorandum on Use of Commercial Cloud Computing Services, dated 9 December 2011.
http://www.disa.mil/Services/DoD-Cloud-Broker/~/media/Files/DISA/Services/Cloud-Broker/Intermin%20Guidance%20Memo%20on%20Use%20of%20Commerical%20Cloud%20Computing%20Services.pdf

➢ Defense Information Systems Agency, DoD Enterprise Cloud Service Broker website.
http://disa.mil/Services/DoD-Cloud-Broker

➢ The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
http://www.gsa.gov/graphics/staffoffices/FedRAMP_Security_Controls_Final.zip

➢ FIPS 199: Standards for Security Categorization of Federal Information and Information Systems, dated February 2004.
http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

➢ NIST SP 500-292: NIST Cloud Computing Reference Architecture, dated September 2011.
http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505

- NIST SP 800-53: Recommended Security Controls for Federal Information Systems and Organizations, Revision 3, dated August 2009. http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/800-53-rev3_markup-rev2-to-rev3_updated-may-01-2010.pdf

Note: http://csrc.nist.gov/publications/PubsSPs.html contains additional documents relating to SP 800-53.

- NIST SP 800-59: Guideline for Identifying an Information System as a National Security System, dated August 2003. http://csrc.nist.gov/publications/nistpubs/800-59/SP800-59.pdf

- NIST SP 800-66, Revision 1: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, dated October 2008. http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf

- NIST SP 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), dated April 2010. http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

- NIST SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing, dated December 2011. http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf